IN THE CLAIMS:

Please amend claims 1, 7, 8, 10, 14, 20, 24, 28, 30, 31, 35 and 36; and

cancel claims 21 and 22 without prejudice and disclaimer as follows.

1. (Currently Amended) A method, comprising:

extracting, at a network element, a routing information from a received message at a border between a first network and a second network;

adding at least one invalid routing entry to first-network routing entries of said routing information to blur or hide an actual number of routing entries which correspond to routing nodes through which said received message has been routed, said first-network routing entries relating to a routing path of said message within said first network;

generating an encrypted routing information by encrypting said at least one invalid routing entry and said first-network routing entries by using an own token at least for each of said first-network routing entries;

replacing said routing information of said received message by said encrypted routing information; and

forwarding said received message with said encrypted routing information to said second network.

2. (Previously Presented) The method according to claim 1, further comprising providing said routing information in a routing header of said message.

3. (Previously Presented) The method according to claim 2, further comprising providing said routing header comprising a record-route header of a session initiation protocol message and a service-route header as specified for the session initiation protocol.

4. (Previously Presented) The method according to claim 1, further comprising processing said routing information using a topology hiding method.

5. (Previously Presented) The method according to claim 4, wherein, in said processing, said topology hiding method is applied in response to a user identity marked with a predetermined information.

6. (Previously Presented) The method according to claim 4, wherein, in said processing, said topology hiding method is applied in response to a network identity.

7. (Currently Amended) The method according to claim 1, further comprising marking said at least one added invalid routing entry.

8. (Currently Amended) The method according to claim 1, further comprising providing each of said first-network routing entries comprising at least one of name and

address information of a network node through which said received message has been routed.

9. (Previously Presented) The method according to claim 1, further comprising providing said border between said first and second networks, wherein said border is defined at a gateway which said message traverses on a connection between said first and second networks.

10. (Currently Amended) An apparatus, comprising:

extracting means for extracting routing information from a received message at a border between a first network and a second network;

adding means for adding at least one invalid routing entry to first-network routing entries of said routing information to blurr or hide an actual number of routing entries which correspond to routing nodes through which said received message has been routed, said first-network routing entries relating to a routing path of said message within said first network;

encrypting means for generating an encrypted routing information by encrypting said at least one invalid routing entry and said first-network routing entries by using an own token at least for each of said first-network routing entries;

replacing means for replacing said routing information of said received message by said encrypted routing information; and

forwarding means for forwarding said received message with said encrypted routing information to said second network.

11-13. (Cancelled)

14. (Currently Amended) A method, comprising:

extracting, at a network element, a routing information from a received message at a border between a first network and a second network;

generating a decrypted and reversed routing information by decrypting a tokenized second-network routing entry relating to a routing path of said message within said second network and by reversing the content of the decrypted second-network routing entry;

replacing said routing information of said received message by said decrypted and reversed routing information; ~~and~~

forwarding said received message with said decrypted and reversed routing information to said second network;

marking a tokenized network routing entry of at least one of an incoming and an outgoing tokenizing network node; and

performing at least one of suppressing said reversing at outgoing tokenizing network nodes and reversing network routing entries at incoming tokenizing network nodes before encryption.

15. (Previously Presented) The method according to claim 14, further comprising:

conveying said routing information in a routing header of said message.

16. (Previously Presented) The method according to claim 15, wherein said routing header comprises at least one of a route header and a via header of a session initiation protocol message.

17. (Previously Presented) The method according to claim 14, further comprising:

using a topology hiding method.

18. (Previously Presented) The method according to claim 17, further comprising applying said topology hiding method in response to a user identity marked with a predetermined information.

19. (Previously Presented) The method according to claim 17, further comprising

applying said topology hiding method in response to a network identity.

20. (Currently Amended) The method according to claim 14, wherein said tokenized second-network routing entry comprises at least one of an encrypted name and encrypted address information of a sequence of network nodes through which said received message has been routed.

21-22. (Cancelled)

23. (Previously Presented) The method according to claim 14, wherein said border between said first and second networks is defined at a gateway which said message traverses on a connection between said first and second networks.

24. (Currently Amended) An apparatus, comprising:

extracting means for extracting a routing information from a received message at a border between a first network and a second network;

decrypting and reversing means for generating a decrypted and reversed routing information by decrypting a tokenized second-network routing entry relating to a routing path of said message within said second network and by reversing the content of the decrypted second-network routing entry;

replacing means for replacing said routing information of said received message by said decrypted and reversed routing information; ~~and~~

forwarding means for forwarding said received message with said decrypted and reversed routing information to said second network;

marking means for marking a tokenized network routing entry of at least one of an incoming and an outgoing tokenizing network node; and

at least one of suppressing means for suppressing said reversing at outgoing tokenizing network nodes and reversing means for reversing network routing entries at incoming tokenizing network nodes before encryption.

25. (Previously Presented) The apparatus according to claim 24, further comprising one of an interrogating call session control function and a topology hiding gateway function.

26. (Previously Presented) The apparatus according to claim 24, wherein said apparatus operates in a packet data network which comprises an Internet protocol multimedia subsystem.

27. (Previously Presented) The apparatus according to claim 24, wherein said apparatus is configured to suppress reversing of said decryptor and reverser when said routing information indicates that said apparatus is an outgoing tokenizing network node.

28. (Currently Amended) The apparatus according to claim 24, wherein said apparatus is configured to reverse network routing entries before encryption when said routing information indicates that said apparatus is an incoming tokenizing apparatus.

29. (Previously Presented) The apparatus according to claim 24, wherein said border between said first and second networks is defined at said apparatus.

30. (Currently Amended) An apparatus, comprising:

an extractor configured to extract a routing information from a received message at a border between a first network and a second network;

an adder, operably connected to said extractor, and configured to add at least one invalid routing entry to first-network routing entries of said routing information to blurr or hide an actual number of routing entries which correspond to routing nodes through which said received message has been routed, said first-network routing entries relating to a routing path of said message within said first network;

an encryptor, operably connected to said extractor, and configured to generate encrypted routing information by encrypting said at least one invalid routing entry and said first-network routing entries by using an own token at least for each of said first-network routing entries;

a replacer, operably connected to said extractor, and configured to replace said routing information of said received message by said encrypted routing information; and

a transmitter, operably connected to said extractor, and configured to forward said received message with said encrypted routing information to said second network.

31. (Currently Amended) An apparatus, comprising:

an extractor configured to extract a routing information from a received message at a border between a first network and a second network;

a decryptor, operably connected to said extractor, and configured to generate a decrypted and reversed routing information by decrypting a tokenized second-network routing entry relating to a routing path of said message within said second network and further configured to reverse the content of the decrypted second-network routing entry;

a replacer, operably connected to said extractor, and configured to replace said routing information of said received message by said decrypted and reversed routing information; ~~and~~

a transmitter, operably connected to said extractor, and configured to forward said received message with said decrypted and reversed routing information to said second network;

a marker configured to mark a tokenized network entry of at least one of an incoming and an outgoing tokenizing network node; and

a processor configured to perform at least one of suppressing said reversing at outgoing tokenizing network nodes and reversing network entries at incoming tokenizing network nodes before encryption.

32. (Previously Presented) The apparatus according to claim 31, further comprising:

one of an interrogating call session control function and a topology hiding gateway function.

33. (Previously Presented) The apparatus according to claim 31, wherein said apparatus operates in a packet data network which comprises an Internet protocol multimedia subsystem.

34. (Previously Presented) The apparatus according to claim 31, wherein said apparatus is configured to suppress reversing of said decrypter when said routing information indicates that said apparatus is an outgoing tokenizing apparatus.

35. (Currently Amended) The apparatus according to claim 31, wherein said apparatus is configured to reverse network routing entries before encryption when said routing information indicates that said apparatus is an incoming tokenizing apparatus.

36. (Currently Amended) The apparatus according to claim 31, wherein said border between said first and second networks is defined at said apparatus.

37. (Previously Presented) The apparatus according to claim 30, wherein said apparatus further comprises one of an interrogating call session control function and a topology hiding gateway function.

38. (Previously Presented) The apparatus according to claim 30, wherein said apparatus operates in a packet data network which comprises an Internet protocol multimedia subsystem.

39. (Previously Presented) The apparatus according to claim 30, wherein said border between said first and second networks is defined at said apparatus.